日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　１月２６日

出願番号
Application Number: 特願２００１－０１９２６７

出願人
Applicant(s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　６月２５日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願

【整理番号】　2022520271

【提出日】　平成13年 1月26日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 13/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　北村　朋彦

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100090446

【弁理士】

【氏名又は名称】　中島　司朗

【先の出願に基づく優先権主張】

【出願番号】　特願2000-237017

【出願日】　平成12年 8月 4日

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9003742

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　システム集積回路

【特許請求の範囲】

【請求項１】　秘密データを格納したメモリデバイスと共に、機器に組み込まれるシステム集積回路であって、

中央処理装置と、

複数の記憶領域を有する記憶手段と、

機器に対する起動操作が操作者によりなされれば、メモリデバイスから秘密データを読み出して、記憶手段における複数領域のうち予め定められた記憶領域に当該秘密データをセットし、その後中央処理装置に対して動作開始を指示する初期化手段と

を備えることを特徴とするシステム集積回路。

【請求項２】　前記機器は、操作者により起動操作がなされた際、外部リセット信号を出力する外部リセット信号出力手段と、

複数のクロックパルスからなるクロック信号を出力するクロック発振手段とを備え、

前記初期化手段は、

外部リセット信号が出力されれば、クロックパルスの波数を計数するカウンタと、

波数の計数値が第１の所定値になれば、メモリデバイスから秘密データを読み出して記憶手段における複数領域のうち、予め定められた記憶領域にセットする読出部と、

波数の計数値が、第１の所定値より大きい第２の所定値になれば、中央処理装置に対して内部リセット信号を出力して動作開始を指示する出力部と

を備えることを特徴とする請求項１記載のシステム集積回路。

【請求項３】　前記秘密データは、機器についての識別情報又は機器を操作する操作者についての識別情報を暗号化して得た暗号化データであり、

システム集積回路は、

読出部により読み出された暗号化データを復号して、元の識別情報を得る復号

化部を備え、

記憶手段における複数の記憶領域のうち、予め定められた記憶領域は、

復号により得られた元の識別情報を格納する

ことを特徴とする請求項１記載のシステム集積回路。

【請求項４】　前記機器においてメモリデバイスは、バスを介してシステム集積回路と接続されており、

前記初期化手段は、機器に対する起動操作が操作者によりなされれば、秘密データをバスに出力するようメモリデバイスに指示し、その後、バスに出力された秘密データを取り込むアクセス制御部を備える

ことを特徴とする請求項１記載のシステム集積回路。

【請求項５】　前記アクセス制御部は、

命令又はデータを読み出す旨が中央処理装置により指示されれば、命令又はデータをバスに出力するようメモリデバイスを制御し、その後、バスに出力された命令又はデータを取り込み、

データを書き込む旨が中央処理装置により指示されれば、データをバスに出力し、その後、バスに出力されたデータを取り込むようメモリデバイスを制御する

ことを特徴とする請求項４記載のシステム集積回路。

【請求項６】　機器においてメモリデバイスは、シリアル線を介してシステム集積回路と接続されており、

前記初期化手段は、機器に対する起動操作が操作者によりなされれば、秘密データをシリアル線に出力するようメモリデバイスに指示し、その後、シリアル線に出力された秘密データを取り込むアクセス制御部を備える

ことを特徴とする請求項１記載のシステム集積回路。

【請求項７】　前記アクセス制御部は、

命令又はデータを読み出す旨が中央処理装置により指示されれば、命令又はデータをシリアル線に出力するようメモリデバイスを制御し、その後、シリアル線に出力された命令又はデータを取り込み、

データを書き込む旨が中央処理装置により指示されれば、データをシリアル線に出力し、その後、シリアル線に出力されたデータを取り込むようメモリデバイ

スを制御する

ことを特徴とする請求項６記載のシステム集積回路。

【請求項８】　システム集積回路はメモリデバイスと共に、機器に組み込まれ、

機器においてメモリデバイスは、バス及びシリアル線を介してシステム集積回路と、接続されており、

前記初期化手段は、機器に対する起動操作が操作者によりなされれば、秘密データをシリアル線に出力するようメモリデバイスに指示し、その後、シリアル線に出力された秘密データを取り込み、

命令又はデータを読み出す旨が中央処理装置により指示されれば、命令又はデータをバスに出力するようメモリデバイスを制御し、その後、バスに出力された命令又はデータを取り込み、

データを書き込む旨が中央処理装置により指示されれば、データをバスに出力し、その後、バスに出力されたデータを取り込むようメモリデバイスを制御するアクセス制御部

を備えることを特徴とする請求項１記載のシステム集積回路。

【請求項９】　前記秘密データは、メモリデバイス固有のデバイス鍵であり、

前記初期化手段は、

機器に対する起動操作が操作者により指示されれば、メモリデバイスからデバイス鍵を読み出して、予め定められた記憶領域に格納し、

前記システム集積回路は、

中央処理装置によりデータ書き込みが命じられれば、書き込むべきデータを、記憶領域に格納されたデバイス鍵を用いて暗号化する暗号化手段と、

暗号化されたデータをメモリデバイスに格納させるよう、メモリデバイスを制御するアクセス制御手段と

を備えることを特徴とする請求項１記載のシステム集積回路。

【請求項１０】　前記アクセス制御手段は、

中央処理装置によりデータ読み出しが命じられれば、暗号化されたデータを読

み込むようメモリデバイスを制御し、

前記システム集積回路は、

読み込まれた暗号化データを復号して、元のデータを得て前記複数の記憶領域における何れかの記憶領域に格納する復号化手段

を備えることを特徴とする請求項９記載のシステム集積回路。

【請求項１１】　秘密データと、複数の命令からなるプログラムとを格納したメモリデバイスに接続されているシステム集積回路であって、

メモリデバイスに格納されたプログラムから命令を順次取り出して、解読する中央処理装置と、

複数の記憶領域を有する記憶手段とを備え、

前記プログラムには、

秘密データを読み込む旨の読出命令が、読み込まれた秘密データを利用した処理を行う旨の命令より前に配置されており、

前記システム集積回路は、

前記中央処理装置が読出命令を解読した際、メモリデバイスから秘密データを読み込んで、複数の記憶領域のうち、予め定められた記憶領域に格納する初期化手段

を備えることを特徴とするシステム集積回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、中央処理装置を初めとする様々な回路が集積されたシステム集積回路に関し、機器に組み込まれて、秘密データを扱う場合の改良に関する。

【０００２】

【従来の技術】

半導体プロセス技術の急速な進歩に伴い、システム集積回路（システムLSI）を内蔵した機器が急速に普及しつつある。システムLSI内蔵型機器は、システムLSIと、1つ以上のメモリデバイスとを含み、セットトップボックス、携帯機器等幅広い分野において、利用されている。かかる機器を具現する回路要素のうち、ロ

ジック部分は、システムLSI内部に実装される。ロジック部分には、中央処理装置(CPU)や、これにより利用されるキャッシュメモリ、レジスタ、トランスポートストリームの多重分離を行うTSデコーダー、MPEGストリームのデコードを行うMPEGデコーダー等がある。これらをLSI内に集積させることにより、ロジック部分の安定動作が保証される。一方、プログラムやデータを格納するROMは、メモリデバイスとしてシステムLSI外部に実装される。データやプログラムがシステムLSI外部に実装されるため、システムLSIに対して改変を加えず、メモリデバイスの格納内容を書き換えることにより、データやプログラムを変更することができる。

【０００３】

セットトップボックスのような機器では、有料放送の受信や有料コンテンツの再生等、ユーザに対する課金が必要になる場合があり、メモリデバイスは機器についての識別情報(機器ID)や、操作者についての識別情報(ユーザID)等秘密扱いが求められるデータ、いわゆる秘密データを格納せねばならない。しかしメモリデバイスの格納内容は、製品の内容を解析する技術、いわゆる”リバース解析”により暴露される危険性がある。そこで従来の機器にあっては、秘密データを暗号化した上でメモリデバイスに格納し、リバース解析が不法に行われることによる秘密データの露見を避けている。

【０００４】

秘密データは暗号化された状態でメモリデバイスに格納されているので、機器に対するハッキング行為を好適に防御することができる。

【０００５】

【発明が解決しようとする課題】

ところでメモリデバイスの格納時において秘密データは万全に暗号化されているとはいえ、メモリデバイスに格納されているプログラムは、暗号化がなされていない場合が多い。CPUのニーモニック表を参照しながらプログラムを逆アセンブルしてゆけば、CPUがどのような処理をするかを伺いしることができる。上述したような機器IDやユーザIDは、CPUの初期動作時にメモリデバイスからシステムLSIに取り込まれることが多いので、CPUの初期動作時において、システムLSI

内のCPUからメモリデバイスに発行される読出コマンドを解析すれば、メモリデバイスに格納されている秘密データが、システムLSIに内蔵されている複数のレジスタ、メモリのうちどれに格納されるかを伺い知ることができる。

【０００６】

秘密データは、復号化部により暗号化が解除された状態でシステムLSI内部のレジスタ、メモリに格納されるので、解読により知り得た読出先を手掛かりにして、より詳細なリバース解析を行えば、暗号化がなされていない状態の秘密データを知得することができる。そうして得た秘密データが、悪意の第三者の手に渡れば、機器に対するハッキング行為が横行する恐れがあり、機器を製造したメーカーや有料放送･有料コンテンツを扱う業者は多大な打撃を被ってしまう。

【０００７】

プログラムを暗号化する等、プログラムの逆アセンブラさえ防止できれば、秘密データの露見は防げるように思える。しかしリバース解析の技術進歩は目覚ましく、CPUが動作を行う際の僅かな痕跡がシステムLSI外部から観測されれば、これを手掛かりとして秘密データの読出先が突き止められることも考えられる。今後、電子マネーの取り扱い等を上述した機器に求める場合には、かかるリバース解析の進歩に対して抜本的な対処をシステムLSIに施しておくことが、システムLSIを製造するメーカーの責務になると考えられる。

【０００８】

本発明の目的は、システムLSI内部におけるCPUの動きがトレースされようとも、メモリデバイスに格納された秘密データの読出先の露見を防ぐシステム集積回路を提供する。

【０００９】

【課題を解決するための手段】

上記目的を達成するため、本発明に係るシステム集積回路は、中央処理装置と、複数の記憶領域を有する記憶手段と、機器に対する起動操作が操作者によりなされれば、メモリデバイスから秘密データを読み出して、記憶手段における複数領域のうち予め定められた記憶領域に当該秘密データをセットし、その後中央処理装置に対して動作開始を指示する初期化手段とを備えることを特徴としている

【００１０】

【発明の実施の形態】

以降図面を参照しながら、システム集積回路（システムLSI）の実施形態について説明する。

（第１実施形態）

本実施形態に係るシステムLSIは、セットトップボックス内に実装されている。図１は、システムLSIを実装したセットトップボックスの内部構成を示す図である。セットトップボックスとは、衛星放送、地上波、有線の何れかから伝送されてくる放送波を受信して、これに含まれているトランスポートストリームの多重分離を行い、更にこれを復号して映像信号、音声信号等を出力する機器であり、テレビジョン受像機やパーソナルコンピュータ等と組み合わせて一般家庭内で用いられる。

【００１１】

図１に示すように、セットトップボックスは、メモリデバイス１０１、１１１、フロントエンド部１０２、周辺デバイス１０３、外部リセット信号発生器１０４、クロック信号発振器１０５を備える。

メモリデバイス１０１、１１１は、機器の動作を実現するプログラムや、データ、機器ID、ユーザIDを格納するためのEEPROM、SDRAMであり、バス、制御線を介してシステムLSIと接続されて二次記憶を構成する。これら各種データのうち、機器ID、ユーザIDは守秘が求められるデータであり、暗号化されてメモリデバイス１０１、１１１に格納される。守秘が求められるデータを暗号化する際のアルゴリズムは、いわゆる”ビットシャッフリング”と呼ばれるものである。このアルゴリズムは、元の機器ID、ユーザIDを構成するビットデータを所定の規則性をもって入れ替えるというものであり、暗号化された機器ID、ユーザIDを、同じ規則性をもって、入れ替えることで、元の機器ID、ユーザIDを得ることができる。

【００１２】

フロントエンド部１０２は、衛星放送アンテナ等が受信した放送波を復調して

、MPEG2規格に規定されたトランスポートストリームをシステムLSIに順次出力する。

周辺デバイス１０３は、フロントパネル、リモコン送受信部を備える。

外部リセット信号発生部１０４は、機器に対する起動操作がなされれば、外部リセット信号を出力する。

【００１３】

クロック信号発振器１０５は、機器に対する起動操作がなされれば、クロック信号を出力する。

セットトップボックスの機能を実現するロジック部分は、このシステムLSI内で実現されるので、セットトップボックス内の基板配線は、極めてシンプルに構成されている。

【００１４】

セットトップボックス内の基板配線がシンプルになった反面、システムLSI内部には、様々な構成要素が高密度に実装されることとなる。図２を参照しながらシステムLSIの内部構成に、どのような構成要素が実装されているかを説明する。図２に示すように、システムLSIは、トランスポートデコーダ１、AVデコーダ２、周辺デバイスインターフェイス３、SRAM４、レジスタファイル５、クロスバススイッチ６、CPU７、命令キャッシュ８、データキャッシュ９、フェッチ部１０、命令デコーダ１１、算術演算回路１２、バスアクセス制御部１３、暗号変換装置１４、及び初期状態管理装置１５からなる。

【００１５】

トランスポートデコーダ１は、フロントエンド部１０２から出力されるトランスポートストリームに対して多重分離を行って、MPEG2規格に規定されたビデオストリーム、オーディオストリームを得て、AVデコーダ２に出力する。

AVデコーダ２は、多重分離されたビデオストリーム－オーディオストリームを復号して、映像信号、音声信号を得る。

【００１６】

周辺デバイスインターフェイス部３は、周辺デバイス１０３におけるフロントパネル、リモコン送受信部とのインターフェイスである。

SRAM４は、メモリデバイス１０１、１１１に格納されているデータの一部を格納する。

レジスタファイル５は、メモリデバイス１０１、１１１に格納されているデータの一部を格納する。メモリデバイス１０１、１１１を二次記憶と称呼したのに対し、これらSRAM４、レジスタファイル５を一次記憶と称する。

【００１７】

クロスバススイッチ６は、データバス、I/Oバス、アドレスバス、命令バスの相互接続を行う。

中央処理装置(CPU)７は、命令についてのキャッシュメモリ(命令キャッシュ８)及びデータについてのキャッシュメモリ(データキャッシュ９)を介してクロスバススイッチ６と接続され、システムLSI内の統合制御を行う。CPU７は、命令キャッシュ８及びデータキャッシュ９を介してメモリデバイス１０１、１１１から命令を取り出すフェッチ部１０と、取り出された命令を解読する命令デコーダ１１と、解読結果に従って、メモリデバイス１０１、１１１からシステム集積回路に読み出されたデータを用いた演算を行う算術演算回路(ALU)１２とを備えている。このことは図２においてCPU７に対応する枠内に示す通りである。

【００１８】

バスアクセス制御部１３は、CPU７からの指示に従ってメモリデバイス１０１、１１１に対する読み書きを行う。以降バスアクセス制御部１３の処理の詳細を、文節(13.i)、(13.ii)、(13.iii)、(13.iv)に分けて説明する。

(13.i)メモリデバイス１０１、１１１からの読み出し時にあたってバスアクセス制御部１３は、二次記憶における格納内容をデータバスに出力するよう、制御線を通じて二次記憶に指示する。データバスに対して格納内容が順次出力されれば、バスアクセス制御部１３はこれら格納内容を順次取り込んでゆき、一次記憶に格納する。

【００１９】

(13.ii)メモリデバイス１０１、１１１への書き込み時にあたってバスアクセス制御部１３は、一次記憶の格納内容をデータバスに順次出力してゆく。それと共に、この格納内容の取り込みを行うよう、制御線を通じてメモリデバイス１０

１、１１１に指示する。かかる指示に従ってメモリデバイス１０１、１１１がデータバスの伝送内容の取り込みを行えば、システムLSIからメモリデバイス１０１、１１１へのデータ書き込みがなされる。

【００２０】

(13.iii)バスアクセス制御部１３によるメモリデバイス１０１、１１１に対する読み書きは、CPU７からの制御に従って行われるが、初期状態管理装置１５からの制御に従って行われる場合もある。つまりCPU７がプログラムを構成するプログラムを読み込む際、又は、プログラムの実行に伴ってデータの読み書きを、メモリデバイス１０１、１１１に対して行う際、バスアクセス制御部１３はCPU７の制御下で、メモリデバイス１０１、１１１のアクセスを行う。一方初期状態管理装置１５の制御下で、メモリデバイス１０１、１１１のアクセスを行うのは、機器の起動時において、メモリデバイス１０１、１１１に格納されている秘密データを読み込むという場合である。

【００２１】

(13.iv)制御線を通じたアクセス指示は、バスアクセス制御部１３がセレクト信号、アドレス信号、コマンド信号といった3種類の信号を出力することによりなされる。セレクト信号は複数のメモリデバイス１０１、１１１のうち、何れを選択するかを示す信号であり、アドレス信号は、セレクト信号により選択されたメモリデバイス１０１、１１１において、何れのアドレスをアクセスするかを示す信号である。コマンド信号は、このアクセスの内容が、読み出し／書き込みの何れであるかを示す。

【００２２】

暗号変換装置１４は、バスアクセス制御部１３によりシステムLSI内部に取り込まれた格納内容が、秘密データであれば、これの暗号化を解除して原データを得た後、一次記憶を構成するキャッシュメモリ、レジスタの何れかに格納させる。一次記憶に秘密データが格納されており、これを書き込むようCPU７から指示されれば、これを暗号化した後にバスアクセス制御部１３に出力し、メモリデバイス１０１、１１１に格納させる。

【００２３】

初期状態管理装置１５は、ユーザにより機器の起動が開始されると、所定の第１期間経過後、メモリデバイス１０１、１１１から機器ID、ユーザIDを読み出すようバスアクセス制御部１３に対して指示を行い、所定の第２期間経過後、初期状態管理装置１５に動作を開始させるべく、内部リセット信号を出力する。上述した第１期間、第２期間の経過を待つのは、セットトップボックス全体のハードウェアを安定させないと、CPUやメモリデバイスの正常動作が保証できないからである。第１期間、第２期間の経過を監視すべく、初期状態管理装置１５はカウンタを有している。

【００２４】

ここで機器の起動とは、機器に供給される電源電圧が所定の電圧値になり、外部リセット信号がLOWからHIGHに立ち上がることをいう。機器に対する電源投入時からしばらくした後、クロック発振器１０５によるクロック信号の発生が開始される。

初期状態管理装置１５の処理の時間的推移を示したのが図３に示すタイミングチャートである。本図の第１段目は、機器外部における電源レベルを示し、第２段目は、外部リセット信号、第３段目はクロックパルス列からなるクロック信号、第４段目、第５段目は、クロックパルスの波数が500回、1000回に達したときに初期状態管理装置１５に内蔵されているカウンタにより出力される通知信号、第６段目は、初期状態管理装置１５に対して発せられる内部リセット信号、第７段目は、バスアクセス制御部１３により発せられる読出信号を示す。

【００２５】

機器の起動操作がなされると、矢印y1に示すように電源が0Vから5Vに立ち上がる。その後、不定期間y2を経た後、クロック発振器１０５は、クロックパルスの出力を開始する。一方、外部リセット信号発生器１０４は、矢印c1に示すように外部リセット信号をLOWからHIGHに立ち上げる。クロックパルスの出力が開始され、外部リセット信号がLOWからHIGHに立ち上がれば、初期状態管理装置１５に内蔵されているカウンタは、クロックパルスのカウントを開始する。カウント開始後、矢印y3に示すようにクロックパルスの波数が500個に達すれば、初期状態管理装置１５内のカウンタは、バスアクセス制御部１３内に通知信号p1を出力す

る。通知信号p1が出力されれば、バスアクセス制御部１３は機器ID、ユーザIDを読み出すようメモリデバイス１０１、１１１に対して、読出信号p3を出力する。

【００２６】

その後、矢印y4に示すように第２期間が経過し、クロックパルスの波数が1000個に達すれば、初期状態管理装置１５内のカウンタは通知信号p2を出力する。バスアクセス制御部１３に内部リセット信号c2をLOWからHIGHに立ち上げる。内部リセット信号c2が立ち上がれば、CPU７はメモリデバイス１０１、１１１からプログラムを構成する命令を読み出して実行するようバスアクセス制御部１３を制御する。

【００２７】

以上のように本実施形態に係るシステムLSIによれば、セットトップボックスの起動にあたって、メモリデバイス１０１、１１１に格納された秘密データをシステムLSI内部に読み込んだ後に、CPU７に動作開始を指示するので、たとえ悪意の第三者がシステムLSI外部からCPU７の動作をトレースしようとしても、秘密データが読み込まれた読出先の所在を悪意の第三者は特定することができない。システムLSI内部における読出先の所在という手掛かりを与えないので、秘密データの読出先を特定しようという悪意の行為の出鼻をくじくことができる。これにより、セットトップボックスに対するハッキング行為を未然に防止することができる。

【００２８】

（第２実施形態）

第１実施形態では、秘密データがバス上を伝送するので、ロジックアナライザ等の機器をバスと接続してバスの伝送内容を観測すれば、暗号化された状態の秘密データを知得することができる。暗号化されているとはいえ、露見された秘密データに対してより詳細なリバース解析を行うことにより、機器ID、ユーザIDが露見されてしまう恐れがある。本実施形態では、バスの伝送内容が観測された場合であっても、秘密データの露見を防ぐような改良を提案する。

【００２９】

第２実施形態における機器の内部構成を図４に示す。本図に示すように、第２

実施形態では、バスアクセス制御部１３とメモリデバイス１０１、１１１とを専用のシリアル線２１で接続している。

第１実施形態では、秘密データを命令、他のデータと同様に扱い、データバス上で伝送させていたが、第２実施形態においてシステムLSIは、秘密データをバス上で伝送させず、この専用のシリアル線２１上で伝送させる。メモリデバイス１０１、１１１からシステムLSIへの秘密データの伝送をシリアル線２１上で行えば、たとえバスの伝送内容がロジックアナライザ等でリバース解析されたとしても、秘密データが露見することはない。シリアル線２１を通じて秘密データを伝送するという点で、守秘性は担保されているので、この実施形態においては、暗号変換装置１４をシステムLSIに設けず、暗号化しない状態で、秘密データをメモリデバイス１０１、１１１に格納してもよい。

【００３０】

（第３実施形態）

第１実施形態では、二次記憶をメモリデバイス１０１、１１１にて構成したが、本実施形態では1つのメモリデバイス１０１にて二次記憶を構成することを提案する。第３実施形態における機器の内部構成を図５に示す。

図５においてシステムLSIは、バス制御を行うバスアクセス制御部１３に代えて、単一のメモリデバイス１０１、１１１に対する制御を行うデバイスアクセス制御部３１を備えている。システムLSIによるメモリデバイス１０１、１１１の制御が制御線を介して行われる点は、第１実施形態と同様である。第１実施形態においてバスアクセス制御部１３は、データ伝送をバス上で行っていたが、第３実施形態におけるデバイスアクセス制御部３１は、データ伝送を、シリアル線３２上で行っている。

【００３１】

システムLSIは単一のメモリデバイス１０１、１１１に対してアクセス制御を行えばよいので、バスを介して制御を行う場合と比較して、システムLSIによる構成の簡易化を具現することができる。またバスに対するリバース解析と比較して、シリアル線に対するリバース解析は困難なので、秘密データを暗号化せずとも、秘密データの露見を効率的に防御することができる。

【００３２】

（第４実施形態）

第１実施形態では、機器の起動時にメモリデバイス１０１、１１１に格納されている秘密データを、システムLSI内部に取り込んだが、第４実施形態ではかかる起動時ではなく、CPU７が秘密データを必要とした場合、メモリデバイス１０１、１１１からシステムLSI内に秘密データを読み込むことを提案する。かかる秘密データの読み込みを実現するため、第１実施形態に示した①メモリデバイス１０１、１１１、②CPU７、③初期状態管理装置１５に対して改良を加えている。以下、第４実施形態に係る改良点について説明してゆく。

【００３３】

①第４実施形態におけるメモリデバイス１０１、１１１が、第１実施形態に示したそれと第１に異なるのは、メモリデバイス１０１、１１１により格納されるプログラム内に、秘密データを複数の記憶領域のうち何れかに読み込む旨の読出命令が存在する点である。第２に異なるのは、このプログラムにおいて、この秘密データについての読出命令が、読み込まれた秘密データを利用する命令より前に配置されている点である。この秘密データについての読出命令が、他の読出命令と異なるのは、秘密データの読出先が明示されていない点である。そのため、たとえメモリデバイス１０１、１１１におけるプログラムを逆アセンブルした者が、この秘密データについての読出命令の存在に気付いたとしても、秘密データが果たしてどの記憶領域に格納されるかを特定することはできない。

【００３４】

②第４実施形態におけるCPU７が、第１実施形態に示したそれと異なるのは、秘密データについての読出命令をメモリデバイス１０１、１１１から読み込んでこれを解読した際、読取要求を初期状態管理装置１５に発行する点である。

③第４実施形態における初期状態管理装置１５は、機器の起動時に秘密データを読み込もうとはせず、読取要求がCPU７から発行された際、メモリデバイス１０１、１１１から秘密データを読み出して、一次記憶のうち、予め定められた記憶領域に設定する。秘密データが一次記憶に格納されれば、この秘密データを用いた処理をCPU７が行う。

【００３５】

以上のように初期状態管理装置１５が、CPU７が読出命令を解読して、秘密データの読取要求を発行した際、秘密データを読み込むので、秘密データの読み込み時期は、機器の起動時に限定されない。そのため悪意の第三者が機器の起動時におけるデータのやりとりを詳細にリバース解析して、秘密データの取得を企てようとも、彼等の執拗なリバース解析をかわすことができる。

【００３６】

尚、本実施形態においてメモリデバイス１０１、１１１とシステムLSIとをシリアル線で接続し、秘密データの伝送をシリアル線を介して行っても良い。

（第５実施形態）

第１実施形態において機器の機能を具現するデータ、プログラムはメモリデバイス１０１、１１１に格納されていることが明らかである。よってこのメモリデバイス１０１、１１１の格納内容がそっくりそのまま他の記録媒体にコピーされれば、機器で使用されているプログラム、データの複製物が容易に作成されてしまう。第１実施形態では、機器ID、ユーザIDのみを暗号化して、メモリデバイス１０１、１１１に格納していたが、第５実施形態では、メモリデバイスに格納されるべき全てのデータを、このメモリデバイス１０１、１１１に固有な暗号鍵（デバイス鍵）を用いて暗号化して格納することにより、デッドコピーの防止を実現している。

【００３７】

図６は、第５実施形態に係るシステムLSIの内部構成を示す図である。図６が図２と異なるのは、図６には暗号変換装置１４は存在せず、システムLSI内部のクロスバススイッチ６と、バスアクセス制御部１３との間に暗号変換装置５０が設けられている。

また第１実施形態において初期状態管理装置１５は、起動時から第１期間経過後に機器ID、ユーザIDをメモリデバイス１０１、１１１から読み出すようバスアクセス制御部１３を制御したが、第５実施形態において初期状態管理装置１５は、同じ第１期間経過後に、暗号化された状態のデバイス鍵を読み出すよう、バスアクセス制御部１３を制御する。

【００３８】

暗号変換装置５０の内部構成を図７に示す。図７に示すように暗号変換装置５０は、デバイス鍵復号部５１、デバイス鍵格納部５２、EX-OR演算部５３、EX-OR演算部５４、EX-OR演算部５５を備える。

デバイス鍵復号部５１は、メモリデバイスから暗号化されたデバイス鍵が読み出されれば、このデバイス鍵を復号して、元のデバイス鍵を得る。

【００３９】

デバイス鍵格納部５２は、デバイス鍵復号部５１により暗号化が解除されたデバイス鍵を格納する。

EX-OR演算部５３は、メモリデバイス１０１、１１１に書き込むべきデータと、デバイス鍵とのEX-OR演算を行い、その結果をバスアクセス制御部１３に出力する。これによりメモリデバイス１０１、１１１に書き込むべきデータは、メモリデバイス１０１、１１１に固有のデバイス鍵にて、暗号化されることになる。

【００４０】

EX-OR演算部５４、５５は、メモリデバイス１０１、１１１から読み出されたデータ又は命令と、デバイス鍵とのEX-OR演算を行い、その結果を一次記憶に出力する。これによりメモリデバイス１０１、１１１内において、データ又は命令がメモリデバイス１０１、１１１に固有なデバイス鍵にて暗号化されていたとしても、メモリデバイス１０１、１１１からのデータ読み出し時において、この暗号化は解除されることになる。

【００４１】

メモリデバイス１０１、１１１に対するデータ読み書きにあたって、EX-OR演算部５３～５５がデバイス鍵と、データとのEX-OR演算を行うのでデータを、メモリデバイス１０１、１１１固有のデバイス鍵により暗号化した状態で、メモリデバイス１０１、１１１に格納しておくことができる。

以上のように本実施形態によれば、メモリデバイス１０１、１１１に格納させるべきデータを、メモリデバイス１０１、１１１に固有なデバイス鍵を用いて暗号化した後、メモリデバイス１０１、１１１に格納するので、たとえ悪意の第三者がメモリデバイス１０１、１１１の格納内容をデッドコピーしたとしても、プ

ログラム、データを他の機器で利用することができない。これによりプログラム、データの守秘性や著作権は好適に保護される。

【００４２】

また暗号化に用いられるデバイス鍵は、CPU７の動作開始に先だって、システムLSI内に取り込まれるので、悪意の第三者がCPU７の動作をトレースしたとしても、デバイス鍵が露見する確率は低い。

尚、本実施形態においてメモリデバイス１０１、１１１とシステムLSIとをシリアル線で接続し、秘密データの伝送をシリアル線を介して行っても良い。

【００４３】

【発明の効果】　以上のように本発明に係るシステム集積回路は、中央処理装置と、複数の記憶領域を有する記憶手段と、機器に対する起動操作が操作者によりなされれば、メモリデバイスから秘密データを読み出して、記憶手段における複数領域のうち予め定められた記憶領域に当該秘密データをセットし、その後中央処理装置に対して動作開始を指示する初期化手段とを備えている。機器の起動にあたって、メモリデバイスに格納された秘密データをシステム集積回路内部に読み込んだ後に、中央処理装置に動作開始を指示するので、たとえ悪意の第三者がシステム集積回路外部から中央処理装置の動作をトレースしようとしても、秘密データが読み込まれた読出先の所在を悪意の第三者は特定することができない。システム集積回路内部における読出先の所在という手掛かりを与えないので、システム集積回路内部における秘密データの読出先を特定しようという悪意の第三者の行為の出鼻をくじくことができる。これにより、機器に対するハッキング行為を未然に防止することができる。

【００４４】

ここで前記機器は、操作者により起動操作がなされた際、外部リセット信号を出力する外部リセット信号出力手段と、複数のクロックパルスからなるクロック信号を出力するクロック発振手段とを備え、前記初期化手段は、外部リセット信号が出力されれば、クロックパルスの波数を計数するカウンタと、波数の計数値が第１の所定値になれば、メモリデバイスから秘密データを読み出して記憶手段における複数領域のうち、予め定められた記憶領域にセットする読出部と、波数

の計数値が、第１の所定値より大きい第２の所定値になれば、中央処理装置に対して内部リセット信号を出力して動作開始を指示する出力部とを備えてもよい。

【００４５】

このシステム集積回路によれば、中央処理装置に対して内部リセット信号を出力する前に、メモリデバイスから秘密データを読み出すので、悪意の第三者がロジックアナライザを用いて中央処理装置の動作を観測したとしても、システムLSIにおける秘密データの読出先が露見することはない。

ここで前記秘密データは、機器についての識別情報又は機器を操作する操作者についての識別情報を暗号化して得た暗号化データであり、システム集積回路は、読出部により読み出された暗号化データを復号して、元の識別情報を得る復号化部を備え、記憶手段における複数の記憶領域のうち、予め定められた記憶領域は、復号により得られた元の識別情報を格納しても良い。

【００４６】

このシステム集積回路によれば、電子マネー等の取り扱い時に利用される秘密データが、暗号化されてメモリデバイスに格納されるので、たとえ悪意の第三者がメモリデバイスの格納内容をデッドコピーしたとしても、悪意の第三者は秘密データを取得することができない。

ここでシステム集積回路はメモリデバイスと共に、機器に組み込まれ、機器においてメモリデバイスは、バス及びシリアル線を介してシステム集積回路と、接続されており、前記初期化手段は、機器に対する起動操作が操作者によりなされれば、秘密データをシリアル線に出力するようメモリデバイスに指示し、その後、シリアル線に出力された秘密データを取り込み、命令又はデータを読み出す旨が中央処理装置により指示されれば、命令又はデータをバスに出力するようメモリデバイスを制御し、その後、バスに出力された命令又はデータを取り込み、データを書き込む旨が中央処理装置により指示されれば、データをバスに出力し、その後、バスに出力されたデータを取り込むようメモリデバイスを制御するアクセス制御部を備えてもよい。

【００４７】

メモリデバイスからシステムLSIへの秘密データの伝送をシリアル線上で行え

ば、たとえバスの伝送内容がロジックアナライザ等でリバース解析されたとしても、秘密データが露見することはない。

ここで前記秘密データは、メモリデバイス固有のデバイス鍵であり、前記初期化手段は、機器に対する起動操作が操作者により指示されれば、メモリデバイスからデバイス鍵を読み出して、予め定められた記憶領域に格納し、前記システム集積回路は、中央処理装置によりデータ書き込みが命じられれば、書き込むべきデータを、記憶領域に格納されたデバイス鍵を用いて暗号化する暗号化手段と、暗号化されたデータをメモリデバイスに格納させるよう、メモリデバイスを制御するアクセス制御手段とを備えてもよい。このシステム集積回路によれば、メモリデバイスに格納させるべきデータを、メモリデバイスに固有なデバイス鍵を用いて暗号化した後、メモリデバイスに格納するので、たとえ悪意の第三者がメモリデバイスの格納内容をデッドコピーしたとしても、プログラム、データを他の機器で利用することができない。これによりプログラム、データの守秘性や著作権は好適に保護される。

【００４８】

また暗号化に用いられるデバイス鍵は、中央処理装置の動作開始に先だって、システム集積回路内に取り込まれるので、悪意の第三者が中央処理装置の動作をトレースしたとしても、デバイス鍵が露見する確率は低い。

ここで秘密データと、複数の命令からなるプログラムとを格納したメモリデバイスに接続されているシステム集積回路であって、メモリデバイスに格納されたプログラムから命令を順次取り出して、解読する中央処理装置と、複数の記憶領域を有する記憶手段とを備え、前記プログラムには、秘密データを読み込む旨の読出命令が、読み込まれた秘密データを利用した処理を行う旨の命令より前に配置されており、前記システム集積回路は、前記中央処理装置が読出命令を解読した際、メモリデバイスから秘密データを読み込んで、複数の記憶領域のうち、予め定められた記憶領域に格納する初期化手段を備えていてもよい。中央処理装置が読出命令を発行した際、秘密データを読み込むので、秘密データの読み込み時期は、機器の起動時に限定されない。そのため悪意の第三者が機器の起動時におけるデータのやりとりを詳細にリバース解析して、秘密データの取得を企てよう

とも、彼等の執拗なリバース解析をかわすことができる。

【図面の簡単な説明】

【図１】

システムLSIを実装したセットトップボックスの内部構成を示す図である。

【図２】

システムLSIの内部構成を示す図である。

【図３】

初期状態管理装置１５の処理の時間的推移を示したタイミングチャートである。

【図４】

第２実施形態におけるシステムLSIの内部構成を示す図である。

【図５】

第３実施形態におけるシステムLSIの内部構成を示す図である。

【図６】

第５実施形態におけるシステムLSIの内部構成を示す図である。

【図７】

第５実施形態においてシステムLSIに設けられた暗号変換装置５０の内部構成を示す図である。

【符号の説明】

１　トランスポートデコーダ
２　AVデコーダ
３　周辺デバイスインターフェイス
４　SRAM
５　レジスタファイル
６　クロスバススイッチ
７　中央処理装置
８　命令キャッシュ
９　データキャッシュ
１０　フェッチ部

１１　命令デコーダ

１２　算術演算回路

１３　バスアクセス制御部

１４　暗号変換装置

１５　初期状態管理装置

２１　シリアル線

３１　デバイスアクセス制御部

３２　シリアル線

５０　暗号変換装置

５１　デバイス鍵復号部

５２　デバイス鍵格納部

５３～５５　EX-OR演算部

１０１、１１１　メモリデバイス

１０２　フロントエンド部

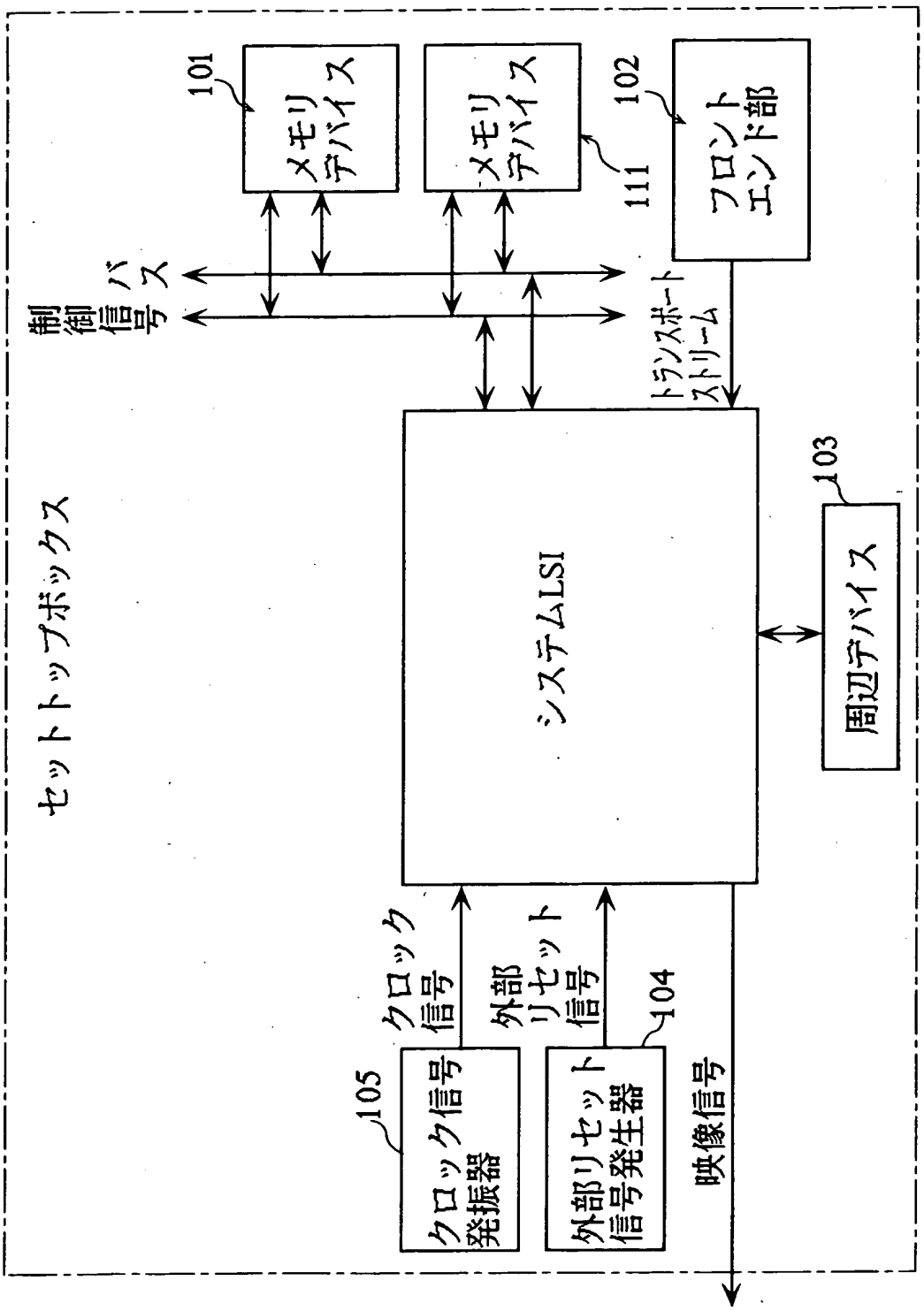
１０３　周辺デバイス

１０４　外部リセット信号発生器

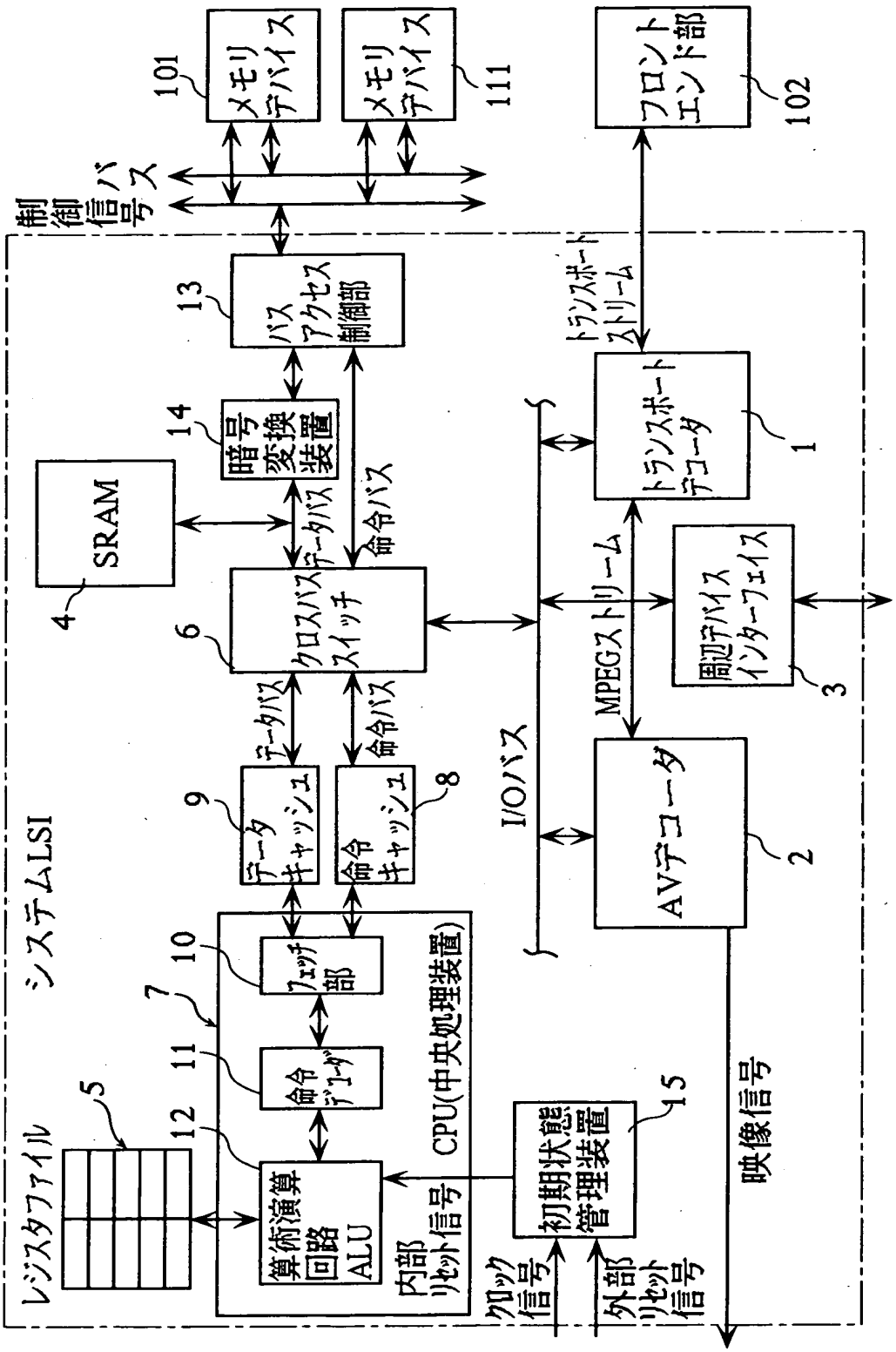
１０５　クロック信号発振器

【書類名】　　図面

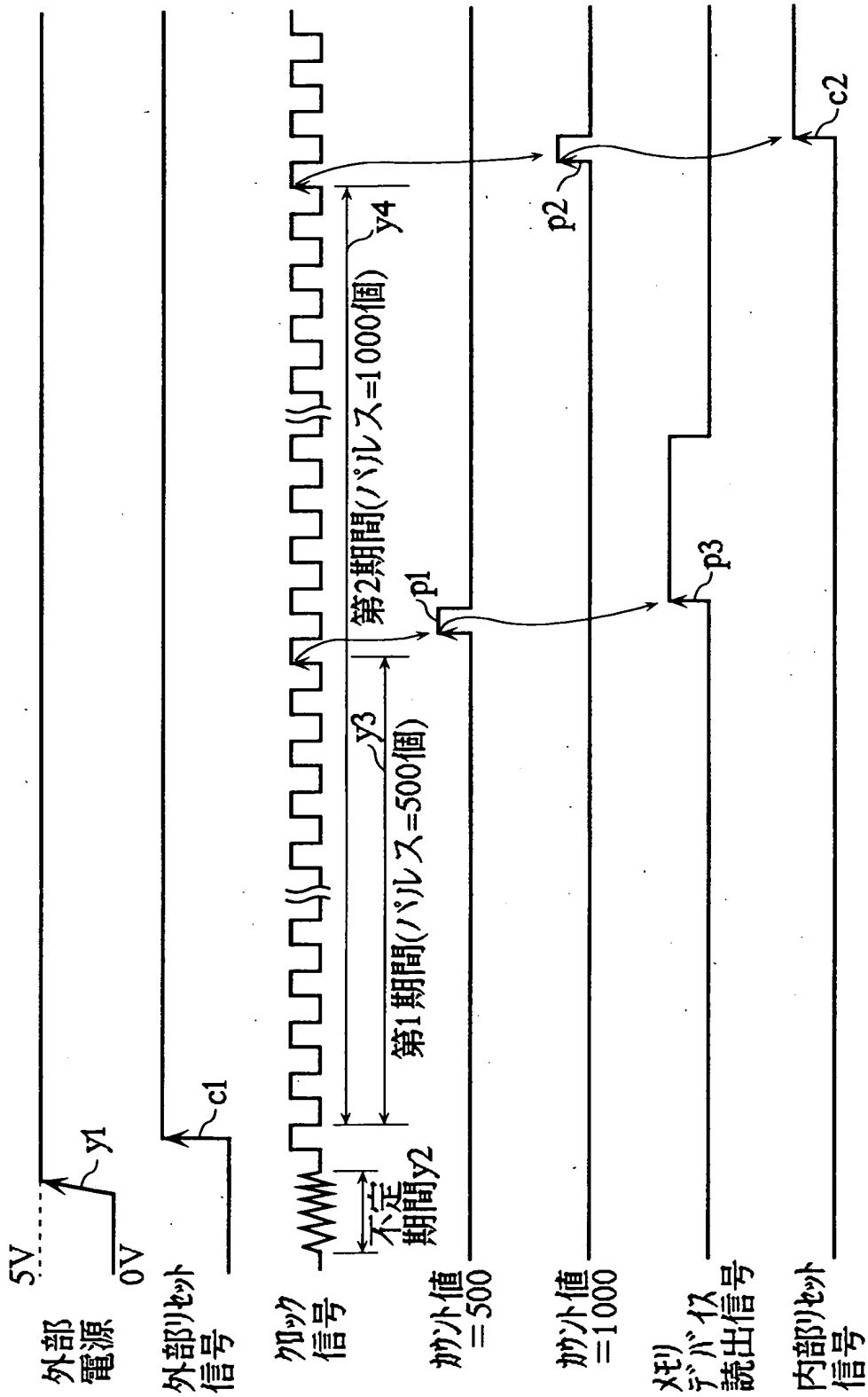
【図１】


セットトップボックス
101
メモリデバイス
メモリデバイス
102
フロントエンド部
111
制御信号バス
トランスポートストリーム
システムLSI
103
周辺デバイス
クロック信号
外部リセット信号
104
クロック信号発振器
105
外部リセット信号発生器
映像信号

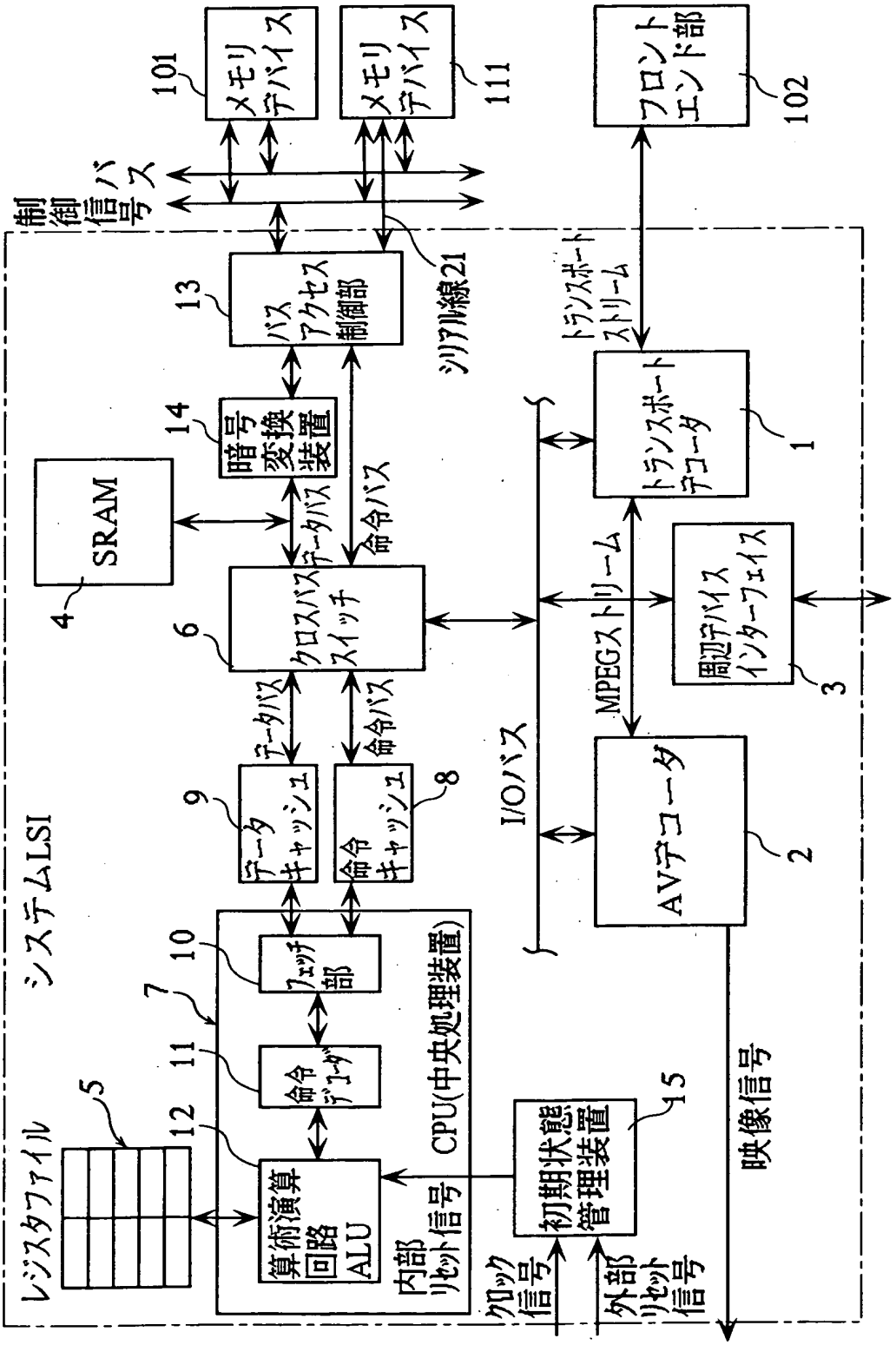
【図２】


メモリデバイス
101
メモリデバイス
111
フロントエンド部
102
制御信号バス
バスアクセス制御部
13
暗号変換装置
14
SRAM
4
データバス
命令バス
クロスバススイッチ
6
トランスポートデコーダ
1
トランスポートストリーム
MPEGストリーム
周辺デバイスインターフェイス
3
I/Oバス
AVデコーダ
2
システムLSI
データキャッシュ
9
命令キャッシュ
8
フェッチ部
10
命令デコーダ
11
CPU(中央処理装置)
7
レジスタファイル
5
算術演算回路ALU
12
内部リセット信号
初期状態管理装置
15
クロック信号
外部リセット信号
映像信号

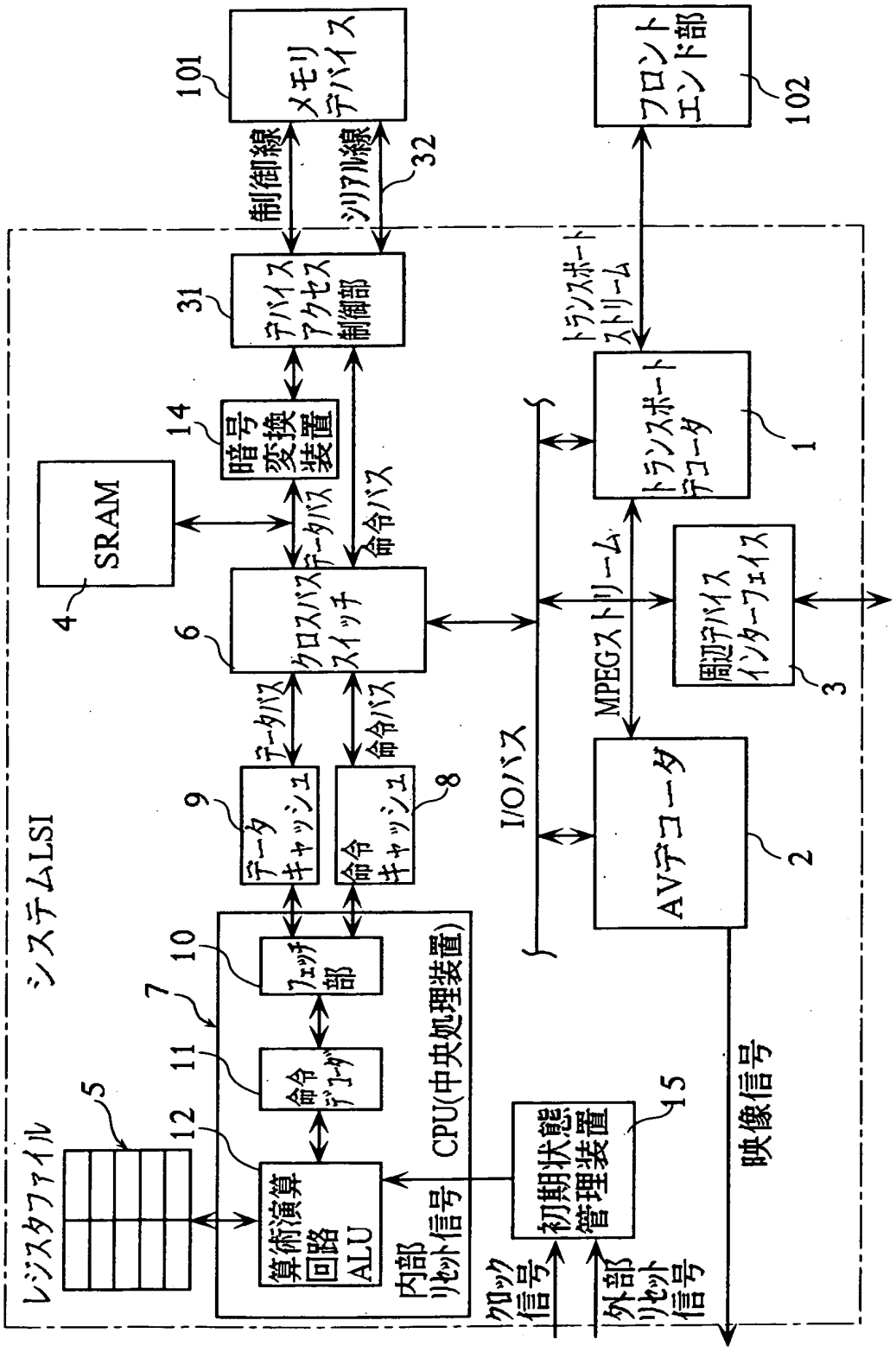
【図３】


外部電源
5V
0V
y1
外部リセット信号
c1
クロック信号
不定期間y2
第1期間(パルス=500個)
y3
第2期間(パルス=1000個)
y4
カウント値=500
カウント値=1000
p1
p2
p3
メモリデバイス読出信号
内部リセット信号
c2

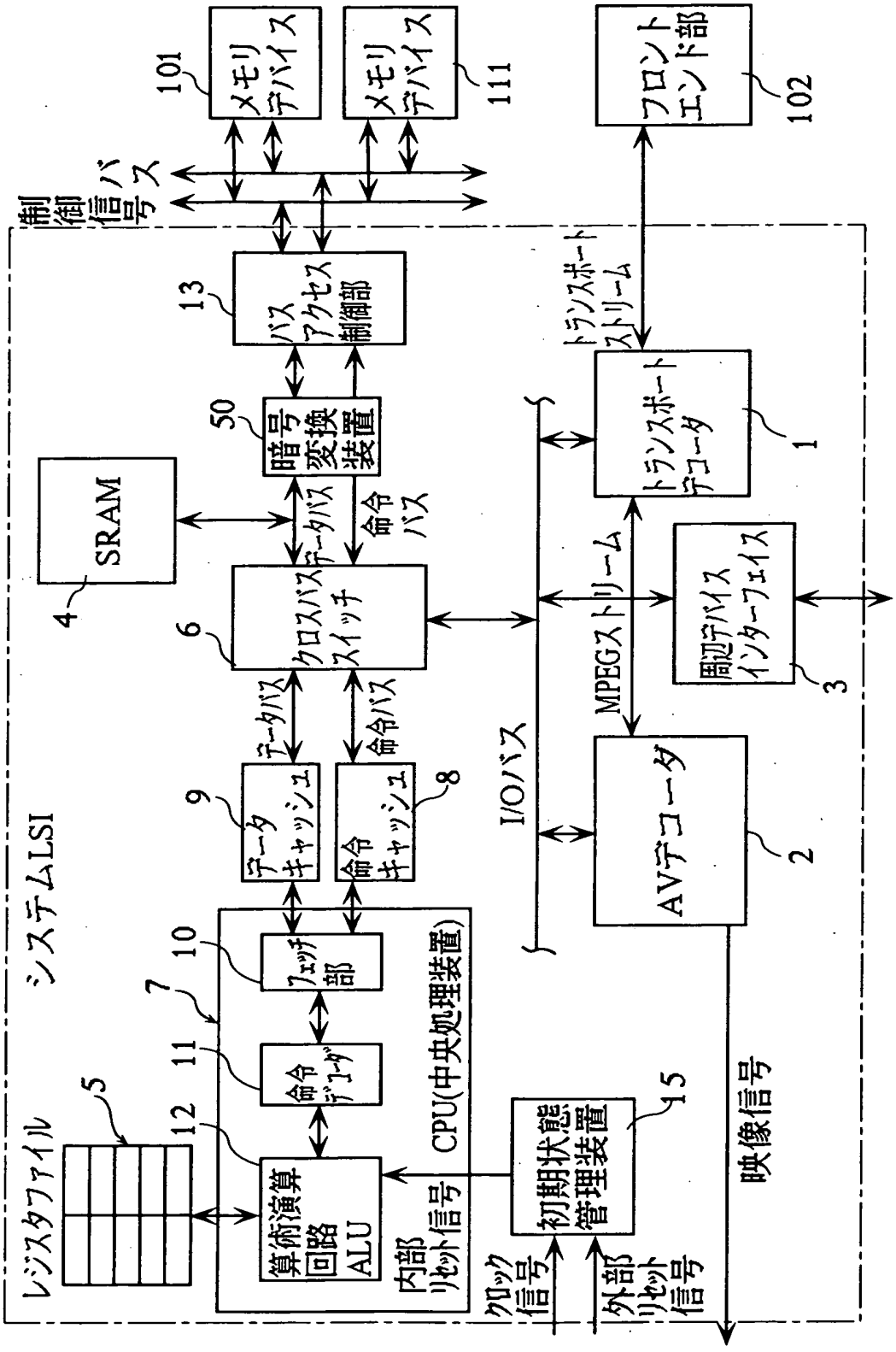
【図４】


システムLSI
CPU(中央処理装置)
レジスタファイル
算術演算回路 ALU
命令デコーダ
フェッチ部
データキャッシュ
命令キャッシュ
内部リセット信号
クロスバススイッチ
データバス
命令バス
SRAM
暗号変換装置
バスアクセス制御部
制御信号バス
メモリデバイス
メモリデバイス
フロントエンド部
シリアル線21
トランスポートストリーム
トランスポートデコーダ
MPEGストリーム
I/Oバス
AVデコーダ
周辺デバイスインターフェイス
初期状態管理装置
クロック信号
外部リセット信号
映像信号
101
111
102
13
14
4
6
9
8
7
10
11
12
5
15
1
2
3

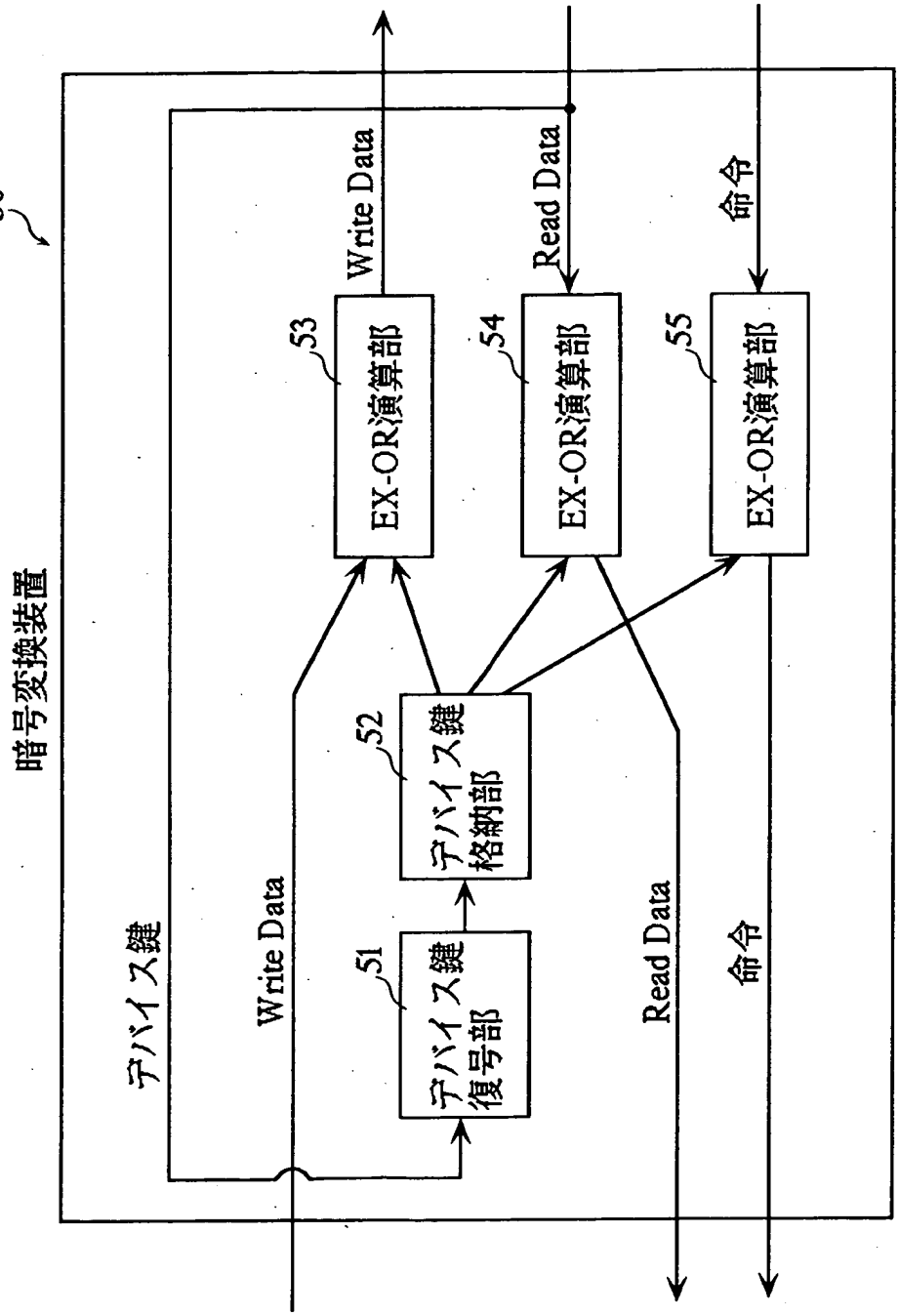
【図５】


システムLSI
101
メモリデバイス
制御線
シリアル線
32
102
フロントエンド部
31
デバイスアクセス制御部
トランスポートストリーム
14
暗号変換装置
SRAM
4
データバス
命令バス
トランスポートデコーダ
1
6
クロスバススイッチ
MPEGストリーム
周辺デバイスインターフェイス
3
I/Oバス
9
データキャッシュ
8
命令キャッシュ
AVデコーダ
2
10
フェッチ部
7
11
命令デコーダ
5
12
レジスタファイル
算術演算回路ALU
CPU(中央処理装置)
内部リセット信号
初期状態管理装置
15
クロック信号
外部リセット信号
映像信号

【図６】


101
メモリデバイス
111
メモリデバイス
102
フロントエンド部
制御信号バス
13
バスアクセス制御部
トランスポートストリーム
50
暗号変換装置
1
トランスポートデコーダ
SRAM
4
データバス
命令バス
MPEGストリーム
周辺デバイスインターフェイス
3
6
クロスバススイッチ
I/Oバス
9
データキャッシュ
命令キャッシュ
8
AVデコーダ
2
システムLSI
10
フェッチ部
7
CPU(中央処理装置)
11
命令デコーダ
5
12
算術演算回路ALU
内部リセット信号
初期状態管理装置
15
映像信号
レジスタファイル
クロック信号
外部リセット信号

【図７】


50
暗号変換装置
デバイス鍵
Write Data
Read Data
命令
51
デバイス鍵復号部
52
デバイス鍵格納部
53
EX-OR演算部
54
EX-OR演算部
55
EX-OR演算部
Write Data
Read Data
命令

【書類名】　要約書

【課題】　内蔵されているCPUの動きがトレースされようとも、メモリデバイスに格納された秘密データの読出先の露見を防ぐシステム集積回路を提供する。

【解決手段】　二次記憶は、秘密データを格納しており、この秘密データは、CPU７により利用されるものである。二次記憶から一次記憶への読み出しはシステム集積回路が組み込まれている機器の起動時に行われる。即ち初期状態管理装置１５は、機器に対する起動操作が操作者によりなされれば、メモリデバイス１０１、１１１から秘密データを読み出して一次記憶における複数領域のうち、何れかにセットする。その後、CPU７に対して動作開始を指示する。たとえCPU７の動作が詳細にリバース解析されようようとも、秘密データの読出先の露見を防ぐことができる。

【選択図】　図１

出証特２００１－３０５９８４５

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社